yubico

Sécurisation des services financiers grâce à une solution de MFA résistant au phishing moderne

Le secteur des services financiers est constamment ciblé par les cyberattaques

Le secteur des services financiers est la cible privilégiée des cybercriminels, entraînant un coût d'environ 5,90 millions de dollars en moyenne pour chaque brèche de données.[1] Les entreprises du secteur financier sont confrontées à des défis en matière de cybersécurité sur deux fronts : côté personnel, elles doivent lutter contre les menaces de phishing ; et côté clients, les banques commerciales et de détail doivent faire face à des menaces de piratage des comptes clients liées aux services bancaires en ligne et mobiles.

Tous les MFA ne se valent pas

Le secteur des services financiers a été l'un des premiers à adopter les solutions d'authentification mobile, telles que les SMS, les OTP et les notifications push. Cependant, bien que toute forme d'authentification multi-facteurs (MFA) soit meilleure qu'un simple mot de passe, tous les MFA ne se valent pas. Les mots de passe sont faciles à pirater, et les MFA sous forme de questions de sécurité, de codes SMS, d'OTP et de notifications push, sont vulnérables face aux attaques par phishing, aux échanges de cartes SIM et aux attaques de type « Man-in-The-Middle ». Les authentificateurs mobiles n'offrent pas non plus une expérience utilisateur optimale.

Le MFA résistant au phishing peut constituer une première ligne de défense solide pour les entreprises de services financiers, assurant la protection des ressources de l'entreprise comme celles des clients.

Qu'est-ce que le MFA résistant au phishing ?

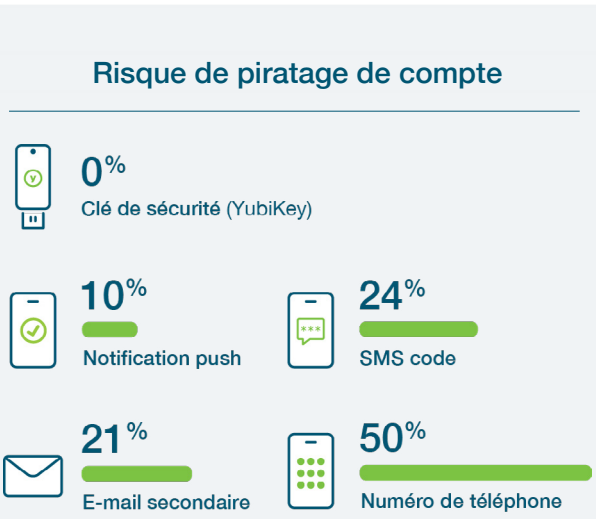
Les processus de MFA résistant au phishing reposent sur la vérification cryptographique entre des appareils ou entre un appareil et un domaine, ce qui les immunise contre les attaques qui tentent de compromettre ou de perturber le processus d'authentification. Selon la Publication spéciale (SP) 800-63 du National Institute of Standards and Technology (NIST), seules deux formes d'authentification répondent actuellement aux exigences en matière de MFA résistant au phishing : les cartes à puce/PIV et le standard d'authentification moderne FIDO2/WebAuthn.

Une solution d'authentification multi-facteurs moderne, sans mot de passe et résistante au phishing avec la YubiKey

Afin de réduire le phishing à l'échelle de l'entreprise et le piratage de comptes clients, Yubico propose la YubiKey, une solution d'authentification multi-facteurs simple, fiable et sans mot de passe.

Des études indépendantes ont montré que les clés YubiKey assurent une sécurité optimale contre les piratages de comptes, préviennent contre les attaques ciblées et offrent un retour sur investissement de 203 %.[2]

Risque de piratage de compte



Recherches menées par Google, NYU et UCSD sur la base de 350 000 tentatives de piratage en situation réelle. Les résultats affichés concernent des attaques ciblées.

Les clés YubiKey sont idéales pour les employés qui travaillent en hybride, à distance ou au bureau, pour les environnements mobiles restreints, pour les postes de travail et appareils partagés, pour les services numériques en contact avec le client et pour les utilisateurs qui ne peuvent pas, ne veulent pas ou n'utilisent pas l'authentification mobile. Elles sont faciles à déployer et à utiliser. Une seule clé YubiKey peut être utilisée sur plusieurs applications, services et appareils classiques et modernes, avec une prise en charge multi-protocoles des cartes à puce, des OTP, d'OpenPGP, de FIDO U2F et de FIDO2/WebAuthn, créant une passerelle pour l'authentification sans mot de passe moderne.

Les clés YubiKey sont également conformes à la norme FIPS 140-2 de l'authentification de niveau 3 (AAL3) NIST SP 800-63B, ainsi qu'aux normes SOX, PCI DSS 4.0, PSD2, RGPD et CFP Circular 2022-04.

Exemples de défis courants dans le secteur financier résolus par la YubiKey

1. Sécurité des employés hybrides et à distance

Le MFA résistant au phishing devrait être l'une des principales exigences des politiques de travail à distance et hybride. La YubiKey fournit une solution de MFA extrêmement fiable et s'intègre facilement aux systèmes et infrastructures existants, y compris aux systèmes de gestion des identités et des accès tels que Microsoft, Okta, Duo, Ping et Hypr. La YubiKey permet aux entreprises du secteur des services financiers de s'assurer que les travailleurs hybrides et à distance disposent d'un accès sécurisé aux ordinateurs, aux VPN et aux gestionnaires de mots de passe, quel que soit leur lieu de travail. Les clés YubiKey peuvent même être utilisées pour générer en toute sécurité des codes secrets à usage unique et limités dans le temps.

2. Sécurité des transactions à haut risque et de grande valeur

Les employés qui effectuent des transactions à haut risque et de grande valeur au quotidien sont souvent la cible de cybercriminels. Grâce aux clés Yubikey, vous bénéficiez d'une authentification multi-facteurs (MFA) solide et moderne, qui renforce l'accès aux systèmes à haut risque et s'assure que seules les personnes autorisées ont accès aux comptes et aux transactions de grande valeur.

3. Sécurité des utilisateurs avec privilèges

Les utilisateurs privilégiés sont des cibles idéales pour les cybercriminels, car ils ont un plus grand accès aux informations sensibles de l'entreprise et des clients. En assurant la mise en application des meilleures pratiques en matière d'authentification sécurisée, et en demandant aux utilisateurs privilégiés d'utiliser des clés de sécurité matérielles résistantes au phishing comme la YubiKey, les entreprises du secteur des services financiers peuvent optimiser la gestion des accès privilégiés et se prémunir contre les attaques ciblées.

4. Sécurité des employés en centres d'appels

Avec un taux de rotation élevé des employés, des pics saisonniers et d'autres dynamiques commerciales difficiles, les environnements de travail des centres d'appels exigent une approche simple et sécurisée pour vérifier l'identité des agents avant de leur donner accès à des systèmes et données critiques. Les clés YubiKey permettent de vérifier l'identité des agents du centre en toute sécurité avant qu'ils n'aient accès aux informations personnelles identifiables et autres données sensibles, ou qu'ils n'effectuent des changements sur le compte d'un client, comme l'augmentation d'une limite de crédit. Contrairement aux téléphones portables, qui peuvent être utilisés pour enregistrer des images des données clients et financières, la YubiKey offre une solution d'authentification sécurisée et conforme.

5. Sécurité des postes de travail/terminaux partagés

Dans les banques et les centres d'appels, il est fréquent pour les employés de travailler sur des postes de travail et des appareils partagés. Les agents passent d'un poste à un autre et les superviseurs se déplacent pour autoriser les transactions. Dans ces environnements, les utilisateurs travaillent souvent à temps partiel, avec un taux de rotation plus élevé, et ils peuvent avoir un sentiment d'engagement moins important envers l'entreprise, ce qui crée des risques de menaces internes. La YubiKey garantit une authentification fiable sur les terminaux d'accès, les postes de travail et les périphériques partagés, et empêche tout accès non autorisé aux systèmes et aux ressources de grande valeur.

6. Sécurité des clients fortunés

En comparaison aux identifiants de connexion, aux SMS et aux codes OTP, les clés YubiKey offrent une sécurité renforcée pour protéger les clients des banques commerciales, ainsi que les comptes bancaires en ligne et mobiles de clients fortunés contre le piratage. Une solution d'authentification fiable et simple à utiliser peut aider les entreprises du secteur des services financiers à acquérir de nouveaux clients et à augmenter la fidélisation. Les clés YubiKey s'intègrent facilement dans les services bancaires en ligne et mobiles. Les entreprises du secteur des services financiers, telles que Vanguard, Morgan Stanley et KeyBank, fournissent aux clients des solutions d'authentification solides avec une prise en charge des clés de sécurité matérielles FIDO.

Obtenez et distribuez facilement des solutions d'authentification YubiKey à grande échelle

Yubico propose des forfaits professionnels flexibles et économiques qui aident les entreprises avec plus de 500 utilisateurs à abandonner les solutions MFA d'ancienne génération compromises et à accélérer l'adoption d'une authentification résistante au phishing à grande échelle.

Avec l'abonnement YubiEnterprise Subscription, les entreprises peuvent bénéficier d'un modèle d'exploitation prévisible, de la flexibilité nécessaire pour répondre aux préférences des utilisateurs avec différentes clés Yubikey disponibles, des mises à niveau vers les dernières clés YubiKey et des mises en œuvre accélérées avec un accès facile aux services de déploiement, à l'assistance prioritaire et à un Customer Success Manager dédié.

Leader de l'authentification fiable

Yubico est l'inventeur principal des standards d'authentification WebAuthn/FIDO2 et U2F adoptés par la FIDO Alliance, et la première entreprise à produire la clé de sécurité U2F et un authentificateur multiprotocole FIDO2.

Les clés YubiKey sont produites aux États-Unis et en Suède, assurant la sécurité et le contrôle qualité de l'ensemble du processus de fabrication.

La série YubiKey 5

De gauche à droite : YubiKey 5 NFC, YubiKey 5C NFC, YubiKey 5Ci, YubiKey 5C, YubiKey 5 Nano et YubiKey 5C Nano

Contactez-nous
yubi.co/contact-fr

En savoir plus
yubi.co/finance

[1] IBM Cost of a Data Breach Report 2023 (Rapport sur le coût d'une brèche de données)

[2] Forrester, Étude Total Economic Impact des clés Yubikey de Yubico

Yubico (Nasdaq First North Growth Market Stockholm : YUBICO) est l'inventeur de la YubiKey, la référence en matière d'authentification multi-facteurs (MFA) résistante au phishing, et un créateur et contributeur des standards d'authentification ouverts FIDO. L'entreprise est un pionnier de l'authentification par passkeys matérielles, avec des clients dans plus de 160 pays. Pour en savoir plus, rendez-vous sur yubico.com